

Serial No. 10/767,454

Reply Dated December 27, 2005

Reply to Office Action Mailed August 26, 2005

Attorney Docket No. 038819.5322US

Both Gabber et al. and the present invention are intended to provide solutions which offer increased privacy for a network user. However, Gabber et al. is concerned in particular with avoiding the transmission of identifying data from a user to a visited web site, while the present invention is concerned with avoiding the storage of sensitive information on the computer used by the user.

The present invention provides a server which provides a secure network browser. A user may use a browser provided on the user's computer to access a web site, which provides secure network browser software for downloading. The user downloads this browser to his or her computer, and uses it to visit the required web sites. According to the present invention, sensitive information may be provided to the visited web site through the secure network browser without fear that sensitive information will be left on the user's computer, possibly for a later user to discover. (It is notable in this regard that, while both Gabber et al. and the present invention use a "proxy server", this is optional in the present invention. (See, page 13, lines 6-15.))

Gabber et al. does not appear to be concerned with or to address the possibility of sensitive data being left on the user's computer. Rather, it is directed to an arrangement for avoiding sending identifying data to visited web sites. This is done by having the user connect to a proxy server. The proxy server receives identifying data from the user, and uses it to generate "anonymized" data in the form of substitute identifiers that are used by the

Serial No. 10/767,454

Reply Dated December 27, 2005

Reply to Office Action Mailed August 26, 2005

Attorney Docket No. 038819.5322US

proxy server to communicate with the site the user wishes to visit. The target site receives the substitute identifiers, and treats them as true user identification. The target site operates as though true identifying data has been received, but the data cannot be traced back to the user since the proxy server of Gabber et al. has generated the substitute identifiers, and the relationship between those identifiers and the true user is not stored in any accessible format.

The present invention as defined in claim 1 differs from the disclosure of Gabber et al. in at least three important respects:

1. *"transmitting...a request for a communications application stored on the server to be downloaded to a terminal connected to the network."*

According to the present invention, this is a request for downloading a secure network browser software from a server to a user's computer.

In the passage referred to in the office action (110a Fig. 2) in this regard, Gabber et al. discloses generating substitute identifiers in the 'server' and sending them to the target web site (col. 5, lines 58 – 66).

Nothing is requested by, or downloaded to, the user's machine in the system of Gabber et al.

2. *"receiving the communications application at the terminal."* As mentioned in the preceding paragraph, nothing is requested by, or downloaded to the user's machine in the system of Gabber et al. The passage referred to in the office action (col. 6, lines 17 – 51) describes

Serial No. 10/767,454

Reply Dated December 27, 2005

Reply to Office Action Mailed August 26, 2005

Attorney Docket No. 038819.5322US

alternative arrangements for generating substitute identifiers either in the user's computer or in the central proxy system. In all cases, there is no communications application downloaded onto the user's computer.

3. *"using the communications application from the terminal over the public data network; wherein the communications application is configured such that user input data, input to the communications application by a user of the terminal, is transmitted into the network without a record of the data being stored at the terminal such that data received at the terminal by the communications application from the network at the request of the user is presented to the user without a record of the data being stored at the terminal".* According to the present invention, this feature defines the operation of the communications application downloaded onto the user's computer. The data input by the user is not stored on the user's computer, and the data received by the user over the network is not stored on the user's computer to avoid detection of sensitive information by a later user of the same computer. According to Gabber et al., substitute identifiers are generated and used to access target web sites, so that no identifying data is sent to the target web site. Gabber et al. is unconcerned with whether data received from the network is stored at

Serial No. 10/767,454

Reply Dated December 27, 2005

Reply to Office Action Mailed August 26, 2005

Attorney Docket No. 038819.5322US

the terminal; rather it is concerned with the level of data sent to the target web site.

Applicant's therefore respectfully submit that Gabber et al. and the present application describe very different, possibly complementary, systems. One (Gabber et al.) avoids detection of a user's identity by target web site by generating and using substitute identifiers in a network server. The other (the present invention) avoids storage of sensitive data on the user's computer by use of a secure browser software downloaded from a network server.

Regarding claims 3 and 4, col. 8, lines 17 – 62 of Gabber et al., describe an interface with software resident on the proxy server. The interface is provided to allow the user to enter data which is then used by the proxy server to generate substitute identifiers. It does not represent a communications application downloaded onto the user's computer.

Regarding claims 5 and 6, Gabber et al. describes the use of a Web Browser, but neither describes nor suggests the downloading of a further web browser from the proxy server to the user's computer for use in communicating with a target web site, as required by the present invention.

Regarding claims 9 and 10, Gabber et al. provides anonymous browsing by generating substitute identifiers which cannot be traced back to the user, and using those identifiers to communicate with a target web site. Insofar as Applicants have been able to determine, however, Gabber et al. does not disclose

Serial No. 10/767,454

Reply Dated December 27, 2005

Reply to Office Action Mailed August 26, 2005

Attorney Docket No. 038819.5322US

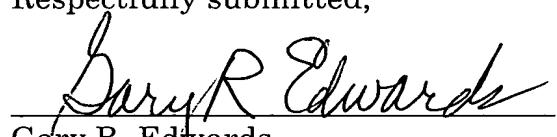
the avoidance of local storage of data received from the network on the user's computer, or the web addresses visited, but rather the avoidance of transmitting sensitive data to the target web site.

In light of the foregoing remarks, this application should be in condition for allowance, and early passage of this case to issue is respectfully requested. If there are any questions regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

If necessary to effect a timely response, this paper should be considered as a petition for an Extension of Time sufficient to effect a timely response, and please charge any deficiency in fees or credit any overpayments to Deposit Account No. 05-1323 (Docket #038819.53225US).

Respectfully submitted,

December 27, 2005

  
\_\_\_\_\_  
Gary R. Edwards

Gary R. Edwards

Registration No. 31,824

CROWELL & MORING LLP  
Intellectual Property Group  
P.O. Box 14300  
Washington, DC 20044-4300  
Telephone No.: (202) 624-2500  
Facsimile No.: (202) 628-8844  
GRE:mdm  
2690474